Journal of Theoretical and Applied Information Technology
31st December 2022. Vol.100. No 24
© 2022 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN INTRUSION DETECTION SYSTEM ON IOT NETWORKS USING HYBRID PCA-GWSO MODEL

JAYABRABU RAMAKRISHNAN[1]

[1]Department of Information Technology and Security

[1]College of Computer Science and Information Technology

[1]Jazan University, Saudi Arabia

Email: [1]jayabrabu@jazanu.edu.sa

ABSTRACT

In any distributed system, network security is a critical concern. For this reason, intrusion detection system (IDS) has been offered to defend the networks against the hostile activity. This analysis aims to create and present an anomaly detection system that can be used to detect intrusions and abnormal activity in the Internet of Things (IoT) networks. The intrusion detection system is critical in identifying diverse attack types on the Internet of Things and improving the IoT's overall functionality. The anomaly identification in the Internet of Things network with glowworm swarm optimization (GWSO) in conjunction with principal components analysis (PCA) was implemented in this work. The proposed framework is a metaheuristic approach-based anomaly detection system that could be used for identifying attacks from the NSL-KDD data set. The anomaly identification process is carried out using the GWSO method based on PCA. The PCA algorithm is employed for feature extraction, and the GWSO technique is employed for classification. Various factors such as accuracy, recall, precision, FAR, and detection rate are assessed in order to conduct a performance analysis. The proposed model achieved 94.14 percent accuracy in the normal class, 95.52 percent accuracy in the DoS class, 93.15 percent accuracy in the R2L class, 93.50 percent accuracy in the probe class, and 88.62 percent accuracy in the U2R class. The detection rate was 94.08 percent, while the false alarm rate (FAR) was 3.41 percent.

Keywords: *IoT, IDS, Anomaly Detection, GWSO, PCA, NSL-KDD Dataset*

1. INTRODUCTION

IoT has proven significant in the real world for the evolution of smartphones, universal and embedded communications, data analysis, and cloud computing [1]. IoT plays an important role in every aspect of our daily lives. It encompasses various industries, such as industrial appliances, autos, sports, healthcare, entertainment, smart homes, etc. The widespread use of the IoT simplifies regular operations, improves how people work with the environment and the world, and increases our social connections between people and objects [2-3].

The IoT is a concept that aims to connect not just humans and computers but also everyday things to the Internet. To accomplish this, things might be outfitted with computation and communication capabilities, effectively projecting the real world to its digital counterpart [4]. In the early period of IoT, transferring information was mostly accomplished over machine-to-machine (M2M) connections. However, the concept has rapidly evolved to include human communications, ushering in a new evolution of the Internet of Everything (IoE) [5]. Though, this causes the expense of security and privacy concerns: if an unapproved, hostile operator has access to our private, tailored data, it can cause significant harm to personal status and security [6].

Furthermore, these systems also integrate resources provided by their manufacturers at diverse stages across the productions and distribution chains. These systems incorporate firmware, fuses, and troubleshooting modes, among other things. This unauthorized access can result in the wrongful appropriation of million dollar worth of copyright and, potentially, the exploitation of these resources to their fullest extent. The consequences of such security flaws could be catastrophic if these devices are widely implemented worldwide [7-9].

The anomaly identification in IoT networks using the GWSO algorithm in conjunction with PCA is proposed in this work. Normally, the GWSO technique is employed mostly for image classification and optimization [10]. It is utilized in this work for intrusion detection in IoT networks. The PCA algorithm is utilized in the feature extraction phase of the dataset. In practice, each attribute has a varied impact on the decision. As a result, this effort began by extracting principal features from the data set utilizing PCA, aiming to minimize the data dimension and shorten the classification time.

This work aimed to create an anomaly detection system that can be used to detect intrusions and strange activity in IoT networks. On the other hand, the research model was a based-on metaheuristic algorithms for detecting anomalies that may be used to identify intrusions on the NSL-KDD dataset. The anomaly identification process uses the GWSO method based on PCA. The PCA algorithm is employed for feature extraction, and the GWSO technique is employed for classification. Hence, the rest of the sections of this paper are: section 2 reviews relevant works on anomaly detections in IoT with various methodologies, section 3 explains the proposed methods, section 4 analyses the achieved results, and section 5 concludes the research.

2. LITERATURE REVIEW

H. H. Dang and D. N. Ha proposed the anomaly identification framework for IoT traffic utilizing the PCA approach, which other researchers then adopted. The PCA approach was used to reduce the number of data dimensions present. A novel formula distance was presented and applied to derive formulae from previous research that was previously published. According to the results of these equations, a novel approach for detecting anomaly in-network traffics was developed and implemented, with adaptable outcomes produced utilizing a novel distance formula that reduced the computing overhead [11]. The computational complexity could have been reduced to achieve a better performance.

H. Ren et al. presented an unsupervised model based on a deep learning system that includes a CNN, and an auto encoder to detect network traffics anomalies early in the process. During the development of the auto-profiling of traffic patterns and abnormal traffics filtering, a D-PACK anomaly traffic detection technique was used. However, the D-PACK only examined initial packets and bytes in each flow to find anomalies as early as possible. The datasets used in the trials were the USTC-TFC and Mirai-CCU databases. After all, was said and done, the model significantly decreased the traffic volume for processing by inspecting fewer packets and total bytes from each packet feasible while maintaining 100 percent accuracy and a minimum of 1 percent false negative and positive rates [12]. This deep learning model could have been developed effectively without any detection delay.

C. Zhaomin et al. proposed a network anomaly identification framework based on the autoencoder technique. In this case, the dimensionality reduction was accomplished using a convolutional autoencoder (CAE). As we all know, compared to a standard autoencoder, this CAE requires far less training time. This model may be used to obtain non-linear correlations between features, which can then be used to improve detection accuracy. In this analysis, the dataset NSL-KDD was applied for evaluations, and this CAE framework outperformed the other models in terms of detection [13]. The autoencoder and CAE can be retrained based on the attack data for improved performance.

According to information entropy, Z. Yansen and L. Jinwei introduced a Multi-level Autoregression approach for network traffic anomaly detections system. The detection of distributed denial-of-service attacks (DDOS) was the primary priority when developing this auto-regression framework. To increase the network traffic detection rate, multi-level autoregression and information entropy models were employed in conjunction with each other to achieve this. The model first computed the network's traffic data entropy/unit-time and utilized zero-mean to obtain the time series of data entropy. It utilized the multi-level auto-regression technique for monitoring sequential entropy, divided the residual with the value of residual averages among the actual value of prediction and entropy, and determined if the anomalies existed by looking for a difference between actual and predicted values of entropy. According to [14], this approach can determine the unknown anomaly traffic but the model can be improved based on the threshold value ratio.

IDS was carried out by A. Maryam and B. Keivan using metaheuristic algorithms such as genetic, glowworm, and particle swarm optimizations. Attacks like DDoS and DoS were used against these approaches, and the lifetime of nodes in the WSN was determined. The PSO algorithm outperformed the genetic algorithm in energy consumption, and the genetic algorithm outperformed the PSO algorithm in permittivity. The GWSO approach has poor performance in permittivity and results in high energy usage [15] compared to other algorithms.

3. MATERIALS AND METHODS

Every distributed system has a substantial security concern, and network security is no exception. In order to defend the network from hostile activity, IDS has been implemented. IDS is used to assist in detecting unauthorized intrusion scenarios by adding an additional layer of protection over networks. Anomaly-based detection and signature-based detection are the two primary strategies used in IDS. The majority of IDS were signature-based frameworks that employ detection criteria. Although, for IDS to be effective, a big distributed network will require a huge number of rules, which could be both time-consumption and expensive.

Additionally, IDS uses the signature of the intrusion to detect malignant activity. If the signatures are not defined sufficiently, hackers might get access to the networks. Unlike human intervention, which has been proposed to overcome these challenges, anomaly-based frameworks are not dependent on human intervention.

The network and host-based intrusion detection system (NIDS and HIDS) were the types of IDS according to detecting intrusions. The HIDS was not ideal for a few IoT system applications with limited functionalities and resources, such as smart home devices. Because the NIDS could track overall network traffics and recognize and block unauthorized and known intrusions, it relies on a hybrid strategy incorporating signature and anomaly-based systems.

Generally, NIDS based on anomaly detections are useful for observing network traffic and recognizing new threats. The signatures-based system could not detect the new intrusion in future network traffic because it is not designed to do so. Because of this, a GWSO algorithm combined with PCA is used to construct the present model, which is designed to detect anomaly-based NIDS-based intrusions.

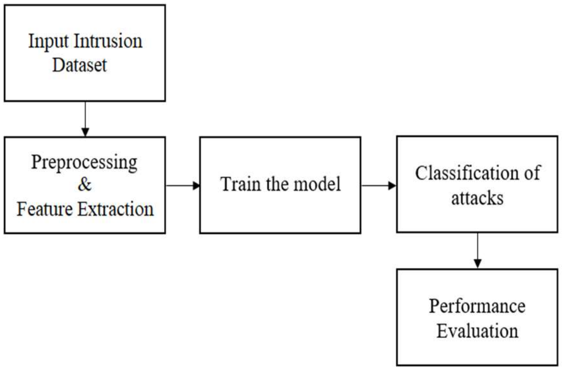

Figure 1: Workflow of the Proposed Model

3.1. PCA

PCA is an approach for dimensionality reduction in which the variables collection of actual correlatives is converted into a set of certain uncorrelated variables, referred to as Principal Component (PC), using a mathematical formula.

These PCs represent the linear combinations of the original variable. The total number of PCs obtained is less than or equal to the whole number of actual variables. As a result, PCA allows for a reduction in complexity. Despite its simplicity, it was regarded as a straightforward yet effective technique for identifying network-based anomalies [16]. Creating the series of linear transformations for the original data with particular connected qualities was the primary principle of PCA. As a result, the matrix of principal components load (PCL) was transformed into a collection of newer information with the fewest features possible to represent the actual data. It was suitable for use in the operation of dimensionality reduction for multi-dimension datasets.

Step 1: Calculate the observation matrix Z for actual data. Observations for x variable θ_1, θ_2, ... θ_x determines the matrix Z after N observations for each variable. All the rows display the numerical estimations of sample information from the data set; column number n refers to the quantity of samples discovered by Equation (1).

$$Z = \begin{bmatrix} Z_{11} & Z_{12} & \cdots & Z_{1x} \\ Z_{21} & Z_{22} & \cdots & Z_{2x} \\ \vdots & \vdots & \ddots & \vdots \\ Z_{n1} & Z_{n2} & \cdots & Z_{nx} \end{bmatrix} \quad (1)$$

Step 2: Organize the data collection and processing into a centralized system for the observation matrix. Calculate the sample mean as well as the standard deviation.

$$\bar{z_b} = \frac{1}{n}\sum_{a=1}^{n} z_{ab} \qquad (2)$$

$$S_b = \sqrt{\frac{1}{n}(z_{ab} - \bar{z_b})^2} \qquad (3)$$

Perform the centralized data process and create a standardized matrix per the formula.

$$\widetilde{z_{ab}} = \frac{z_{ab}-\bar{z}_b}{S_b} \ (a = 1,2,\dots,n, b = 1,2,\dots,x) \ (4)$$

Step 3: Preparation of a sample correlations matrix using the equation,

$$W = \frac{1}{n}\tilde{Z}^T\tilde{Z} \qquad (5)$$

According to equation (6), the computations of all the elements in *W* was as follows,

$$w_{ab} = \frac{\sum_{k=1}^{n}(z_{ka}-\bar{z}_a)(z_{kb}-\bar{z}_b)}{\sqrt{\sum_{k=1}^{n}(z_{ka}-\bar{z}_a)^2\sum_{k=1}^{n}(z_{kb}-\bar{z}_b)^2}} \qquad (6)$$

Step 4: Evaluate the Eigen vectors and eigen values of *W*, and determine W's *x* characteristic value, which is as follows: $\lambda_1 \geq \lambda_2 \geq .... \geq \lambda_x \geq 0$. As a result, using the formula, determine the rate of contribution of each primary component.

$$r_a = \frac{\lambda_a}{\lambda_1+\lambda_2 ... +\lambda_x}(a = 1,2,\dots,x) \qquad (7)$$

Select the higher *p* that achieves 85 percent and encounters $\lambda_{p+1} < 1$ as PCA results and use it as a starting point. If the values of the descending order features were $\lambda_1, \lambda_2, ..., \lambda_x$, then evaluate eigen vectors $e_1, e_2, ..., e_x$. Select the best feature vector *p* for inclusion in the PCL.

$$L_{x\times p} = (e_1, e_2, \dots, e_p) \qquad (8)$$

Step 5: Formulate a linear transformation for original data based on matrix of PCL $L_{x\times p}$ and Equ (9) to generate newer principal variable, such as w_1, w_2, …, w_p.

$$\begin{bmatrix} w_1 \\ \vdots \\ w_p \end{bmatrix} = L_{x\times p}^T \begin{bmatrix} \theta_1 \\ \vdots \\ \theta_p \end{bmatrix} \qquad (9)$$

After the linear transformation, the matrix dimension reduced from *x* to '*p*', which resulted in a considerable reduction in the volume of the sampled data.

3.2. GWSO

This approach was inspired by the ideology of glowworm foraging or courtship behaviours, in which they emit a bright glow to attract companions. A certain amount of luciferin is present in each glowworm in the GWSO, which defines the luminance intensity. During an algorithmic operation procedure, every glowworm moves in the direction of its neighbour, which is more luminous than it is. Local data was used to guide these actions, allowing the swarm to divide into discrete subgroups that combined to perform multimodal functions through various optima. Generally, GWSO is divided into four stages: glowworms dissemination, luciferin update, glowworm movements, and neighbourhood range update [17].

3.2.1 Glowworm Distribution

A set of *n* glowworms is randomly scattered over the search space, with each glowworm appearing in a different location. Luciferin l_o is carried by each glowworm in the same amount.

3.2.2 Luciferin Update

This step was predicated on the importance of previous separate luciferin levels and objective functions in determining the outcome. The luciferin update rule is,

$$l_g(i) = (1-\rho)l_{g-1}(i-1) + \gamma H(x_g(i)) \ (10)$$

The luciferin value at the i^{th} iteration was denoted by $l_g(i)$. The luciferin enhancement factor and decay were denoted by γ and ρ, respectively, and the value of objective functions at the glowworm's location was denoted by $H(x_g(i))$.

3.2.3 Glowworm Movement Stage

This stage is characterized by each glowworm drawing closer to a neighbour with a higher brightness than itself, according to a probabilistic manner. In the case of each glowing worm *g*, the probability of moving toward its neighbour *h* was

$$p_{gh}(i) = \frac{(l_h(i)-l_g(i))}{\sum_{j\in N_g(i)}(l_j(i)-l_g(i))} \qquad (11)$$

where, $h \in N_g(i)$, $N_g(i)$ was the set that might be ensured by

$$h \in N_g(i), N_g(i) = \{h: d_{gh}(i) < r_d^g(i); l_g(i) < l_h(i)\} \qquad (12)$$

where $d_{gh}(i)$ represents the Euclidean distances between glowworm *h* and *g* at the i^{th} iterations and $r_d^g(i)$ represents the variables neighborhood ranges associated with glowworms *g* at the i^{th} iterations. As a result, the glowworm's movement process was denoted by,

$$x_g(i+1) = x_g(i) + si * \left(\frac{x_h(i)-x_g(i)}{\|x_h(i)-x_g(i)\|}\right) \qquad (13)$$

here, $x_g(i)\epsilon R^m$ denoted glowworms g's position at i^{th} iterations in an m-dimension space R^m, $\|x_h(i) - x_g(i)\|$ denoted norm operators of Euclidean, and the si (>0) denotes the size of steps.

3.2.4 Neighborhood Range Update

The neighborhood domains of all the glowworms were presented in the generations, taking into account r_0 as the initial neighborhood domains for all the glowworms and the neighborhood domains of all the glowworms.

$$r_d^g(i+1) = \min\left\{r_s, max\{0, r_d^g(i) + \beta(n_i - N_g(i)\}\right\} \quad (14)$$

here β represents constant, r_s denotes sensory range of the glowworms, n_i is the control parameters for neighborhood count, and N_g (i) denotes the number of neighbourhoods that had been set [18].

3.2.5 Pseudocode of GWSO

```
Initialize
Set generations A = 1; population size = n; problem dimension = m;
Step size = si(0); initialize parameters β; γ and r0; initialize luciferin = $l_0$;
Glowworm distribution
Glowworms randomly dispersed in search space.
All glowworms carry the same luciferin $l_0$ and initial neighborhood domain radius $r_0$
While A < max generation do
for g = 1: n (every glowworm) do
Updation of luciferin using Eq. (10)
Verifying neighbors set using Eq. (12);
Compute the movement probability using equation (11);
Select the neighbor h by probabilistic mechanisms;
Glowworm g shifts over h using Eq. (13);
Updation of neighborhood range using Eq. (14);
End for
End while
Outputs and end of the algorithm
```

The anomaly identification in the Internet of Things networks using the GWSO algorithm in conjunction with PCA is proposed in this work. Typically, the GWSO algorithm is employed primarily for image classifications and optimizations. It is utilized in this analysis for intrusion detection in Internet of Things networks. The PCA algorithm is utilized in the feature extraction phase of the dataset. In practice, each attribute has a varied impact on the decision. As a result, this work began by extracting key attributes from the data set with PCA, aiming to minimize the data dimension and shorten the classification time.

4. EXPERIMENTAL ANALYSIS

This proposed model uses MATLAB 2018a for its implementation and evaluation, performed on a laptop equipped with a CPU running at 2.80 GHz and 8 GB of RAM. The proposed approach will be evaluated based on the parameters of the results like accuracy, FAR, detection rate, recall, and precision. The presented GWSO-PCA technique's performance will be compared to that of other methodologies like ANN, BPNN, SVM, and PSO, as well as other methodologies like BPNN and PSO.

4.1. Dataset

The NSL-KDD dataset was evolved from the KDD99 data set in order to overcome the limitations of the KDD99 dataset. The general public can access the dataset through its official website. Duplicate records were eliminated from the training and test sets at the beginning of the process. Once this is done, many records are chosen from the original KDD-99 to acquire precise outcomes for classification frameworks. Then, it eliminates the problems of the imbalanced distributions of probability from the equation of probability distribution. There are 125,973 training samples and 22,544 testing cases in the NSL-KDD data collection, including 41 features, 38 constant attributes, and 3 class attributes (discrete values). Six sequential variables were eliminated from consideration because they were majorly 0s. On the one hand, there are 38 sets in the testing dataset, suggesting that there were no intrusions into the testing data during training; on the other hand, there were 23 possible labels in the training dataset. There were 21 classes spread throughout 38 testing and 23 training classes; two classes were only held during training, and 17 classes were out of the ordinary for testing knowledge.

Overall, 16.6 percent of the testing dataset samples were classes that were great for the testing dataset but were not present while the training phase of the experiment. The classifications become more complex due to the distribution variation of the classes. Training and testing classes were related to one of five types of attacks: DoS, Normal, R2L, PROBE, and U2R. Normal is the most common class. Aside from the Normal classification, each of the other classifications is identical to an incursion, which implies that no intrusions were shown. These classes were still valuable in understanding the notion of IDS. They are very imbalanced, as they contain enough cases to provide statistically significant findings in each class.

Probe: The term probe refers to when the intruders attempt to obtain information about the target networks through networks and behavior of hosts scanning (i.e., port scanning).

DoS: Once the intruders prevent legitimate users from logging into a specific service or machine, this is referred to as denial of service (DoS).

U2R: When the intruders attempt for extending a minimum user's advantages to root accesses, this is called U2R. (Through stolen data or malware injection).

R2L: When the intruders gain access to the target system by wirelessly impersonating current local users, this is R2L. The U2R and R2L attacks were two major offensive attacks defined as imitating a typical user's actions, and they are classified.

Table 1: Traffic Distributions of NSL-KDD

Traffics	Training	Test
DoS	45927	7458
U2R	52	200
Normal	67343	9711
R2L	995	2421
Probe	11656	2754
Total	125973	22544

4.2. Evaluation of Performance

The model's accuracy was only a subset of the system's overall performance. It was a performance indicator that may be used to evaluate classification techniques in general. The following expression is used to calculate the accuracy of the accuracy computation:

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{15}$$

Precision can be defined as a high rate of success in predicting the future. It is defined as the ratio of correctly predicted positive observations to the total expected positive value of the predicted positive.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \tag{16}$$

The term "sensitivity" refers to the ability to recall information. It is defined as the ratio of all the observations in the actual class to the properly predicted positive value.

$$\text{Recall} = \frac{\text{TP}}{(\text{TP+FN})} \tag{17}$$

The detection rate (DR) is a measure of the number of intrusion instances that have been detected. It indicates the total count of appropriate predictions of the positive class generated as a percentage of the total number of predictions made. It is necessary to calculate the DR in order to satisfy the accompanying condition (18).

$$\text{DR} = \frac{\text{TP}}{\text{TP+FN}} \tag{18}$$

The False Alarm Rate (FAR), as defined by Equation (19), is the normal data proportion mistakenly classified as attack activities. It was further referred to as the FP ratio.

$$\text{FAR} = \frac{\text{FP}}{\text{TN+FP}} \tag{19}$$

The presented model is evaluated based on the criteria listed above, which depend on the identifications of the intrusions in the data set used in the evaluation. In any scenario, accuracy was a measurement of correct identifications; DR denotes the rate at which the classifier detects intrusions; FAR denotes the proportions of normal cases that were misclassified, and recall denotes the number of attacks that the model detected. The precision is what determines whether or not the attacks returned are correct. For validating the GWSO-PCA approach and comparing it with other present approaches, it is necessary to test the performance evaluations of diverse outcome parameters to compare them with one another.

Table 2: Dataset Traffic Distribution Results of The Proposed Model

Attacks	Accuracy	FAR	Precision	Recall
U2R	92.68	3.1	92.30	93.79
DoS	92.22	1.2	94.22	95.71
R2L	90.41	8.7	89.74	91.12
Probe	94.89	1.4	93.47	93.45

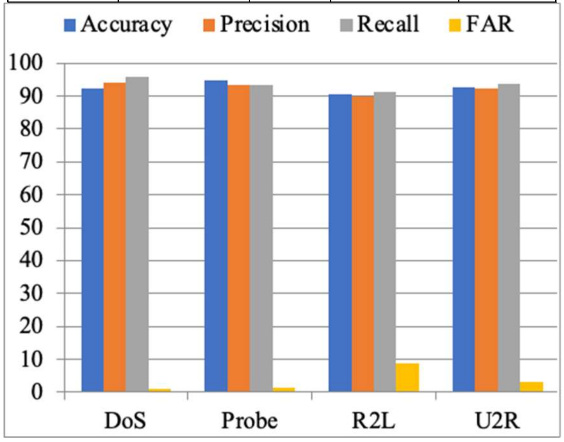

Figure 2: Plot for GWSO-PCA Performances

The experimental evaluations of the proposed approach, which was performed on the NSL-KDD data set, are depicted in table 2. All the classes of intrusion were evaluated with accuracy, recall, FAR, and precision. The performance analysis of the presented model is depicted in graphical form in figure 2. Previously, as stated, this model's performances were compared to other existing approaches such as artificial neural networks (ANN), back-propagation neural networks (BPNN), support vector machines (SVM), and particles swarm optimizations (PSO), as represented in table 3. In this section, classification accuracy was validated by comparing under the plot shown in figure 3.

Table 3: Classification accuracy comparison

Model	Normal	DoS	R2L	Probe	U2R
PSO	92.45	94.30	90.53	93.27	86.26
BPNN	93.24	91.07	92.80	93.98	84.38
ANN	90.40	89.23	80.87	89.10	62.02
SVM	91.72	85.37	88.21	86.75	78.85
GWSO-PCA	94.14	95.52	93.15	93.50	88.62

Compared to the other methodologies, the presented GWSO-PCA approach outperformed them in most performances. In normal cases, the GWSO-PCA acquired 0.9 to 3.7 percent more detections; for DoS attacks, the proposed model obtained 1.2 to 10.15 percent highest detection; in R2L class, the model acquired 2.7 to 14 percent additional detections; in the probe case, the model acquired 0.2 to 6.75 percent more precise detections; and in U2R, the proposed model obtained 2.3 to 26 percent higher detection.

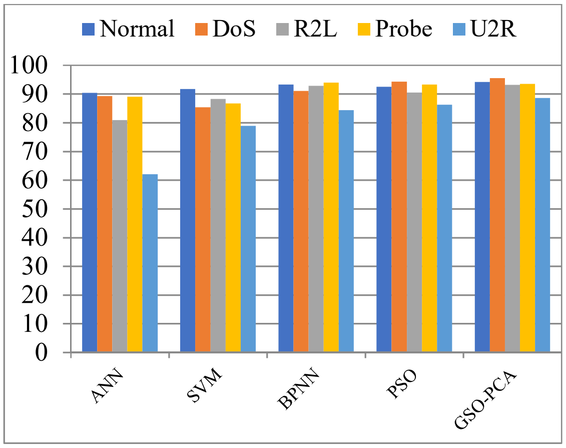

Figure 3: Classification Accuracy Comparison

Table 4 presents the results of a comparison between DR and FAR. Figure 4 depicts a graphical representation of the comparison when appropriate.

Table 4: Comparison of FAR and Detection Rate

Method	FAR (%)	Detection Rate (%)
ANN	5.06	86.52
PSO	3.98	93.60
BPNN	4.55	91.84
SVM	4.73	88.30
GWSO-PCA	3.41	94.08

The proposed model had a higher detection rate and a lower FAR than existing strategies. Both in terms of detection rate and FAR, the PSO came quite near to the findings of the presented model. While the ANN has shown the poorest performance, the proposed model demonstrated the best performance, achieving 94.08 percent DR and 3.41 percent FAR. In comparison, the ANN demonstrated the worse performance while achieving 5.06 percent FAR. The GWSO-PCA model has produced an increase in the detection rate of 0.4 to 7.5 percent and a decrease in FAR of 0.5 to 1.6 percent.

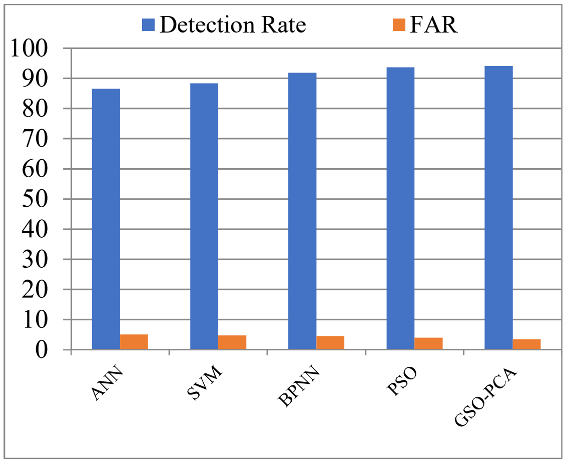

Figure 4: Comparison of FAR and DR

The authors in [11] used only the PCA approach for detecting the anomalies in the network, but in this research model the PCA was integrated with GWSO for improved performance. According to results of the existing works [13-15], the research model has performed better dataset distribution and obtained higher results in terms of detecting intrusions in the network.

According to the obtained results, the objective of this proposed research has been satisfied. The primary aim of this research model was to detect the intrusions and abnormal activities present in the IoT network. The research model has obtained better detection rate with 94.08% and lowest FAR rate with 3.41%, which represents that the model is effective and secure against intrusions. The limitations of this work are, the research model detects the intrusions, instead it requires higher memory for processing the data and the computational complexity was higher.

5. CONCLUSION

The anomaly identification in the Internet of Things networks using the GWSO algorithm in conjunction with PCA was proposed in this research. Generally, the GWSO method was mostly utilized for optimization and image classification purposes. It was applied in this work to the detection of intrusions into IoT networks. The PCA extracted features from the dataset throughout the feature extraction phase. The proposed model was created to improve the performance of IoT networks when it comes to identifying anomalies. The NSL-KDD dataset was utilized for attack classification and detection. Utilizing this data set, the proposed approach was trained and tested in order to determine its overall performance. A powerful feature extraction algorithm, the PCA, was utilized to extract the dataset's attributes, and the GWSO was utilized to detect and classify the various types of intrusions in the data set. Compared to the other works discussed in the literature review, the research model PCA-GWSO has outperformed in detecting intrusions and anomalies with better performances.

Various performances, including accuracy, FAR, recall, detection rate, and precision, were examined to determine overall performance. The proposed model achieved 94.14 percent accuracy in the normal class, 95.52 percent accuracy in the DoS class, 93.15 percent accuracy in the R2L class, 93.50 percent accuracy in the probe class, and 88.62 percent accuracy in the U2R class. The DR was 94.08 percent, while the FAR was 3.41 percent. Although the presented model did not attain the best overall performance compared to other current approaches such as ANN, SVM, BPNN, and PSO, it did perform well in every parameter compared to them.

In future, it is possible to implement the proposed model using various datasets on various network platforms such as WSN, MANET, and others. Additionally, a new hybrid system utilizing deep learning techniques could be developed to improve the DR and reduce the FAR.

REFERENCES:

[1] S. Mansour and B. Hamid, "A hybrid intrusion detection architecture for internet of things," *in Proceedings of IST'2016*, Tehran, Iran, 2016, pp. 601-606.

[2] N. Mehdi, S. Vijay and B. Roksana, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," *in Proceedings of ARES,* Salzburg, Austria, 2016, pp. 147-156.

[3] M. Sailaja, K. R. Kiran, R. M. P. Sita and P. P. E. S. N. Krishna, "A novel approach for intrusion detection using swarm intelligence," *in Proceedings of InConINDIA*, Visakhapatnam, India, Vol. 132, No. 1, 2012, pp. 469-79.

[4] H. A. Mohammed, A. D. A. M. Bahaa, I. Alyani and F. Z. Mohamad, "A new intrusion detection system based on fast learning network and particle swarm optimization," *IEEE Access*, Vol. 6, No. 1, 2016, pp. 20255-61.

[5] K. S. Nilesh and M. Indrajit, "Machine learning based anomaly detection for IoT network," *in Proc ICOEI2020*, Tirunelveli, India, 2020, pp. 787-794.

[6] M. Savic, M. Lukic, D. Danilovic, Z. Bodroski, D. Bajović *et al.*, "Deep learning anomaly detection for cellular IoT with applications in smart logistics," *IEEE Access*, Vol. 9, 2021, pp. 59406-59419.

[7] C. Andrew, M. Goksel and F. Zhong, "Anomaly detection for IoT time-series data: a survey," *IEEE Internet of Things Journal*, Vol. 7, No. 7, 2020, pp. 6481-6494.

[8] E. Sohaila, B. May, A. N. Noora, C. Zina and E. Aiman, "Machine learning techniques for network anomaly detection: a survey," *in Proceedings of ICIoT*, Doha, Qatar, 2020, pp. 156-162.

[9] B. Hussain, Q. Du, A. Imran and M. A. Imran, "Artificial intelligence-powered mobile edge computing-based anomaly detection in cellular networks," *IEEE Transactions on Industrial Informatics*, Vol. 16, No. 8, 2018, pp. 4986-4996.

[10] S. H. Haji and S. Y. Ameen, "Attack and anomaly detection in IoT networks using machine learning techniques: a review," *Asian Journal of Research in Computer Science*, Vol. 9, No. 2, 2021, pp. 30-46.

[11] H. H. Dang and D. N. Ha, "A PCA-based method for IoT network traffic anomaly detection," *in Proc. ICACT*, Chuncheon, South Korea, 2018, pp. 381-386.

[12] H. Ren, P. Min-C, H. Chien-W, L. Po-C and N. Van-L, "An unsupervised deep learning model for early network traffic anomaly detection,"

IEEE Access, Vol. 8, No. 1, 2020, pp. 30387-99.

[13] C. Zhaomin, K. Y. Chai, S. L. Bu and T. L. Chiew, "Autoencoder-based network anomaly detection," *in Proceedings of WTS*, Phoenix, AZ, USA, 2018, pp. 1-5.

[14] Z. Yansen and L. Jinwei, "Research of network traffic anomaly detection model based on multi-level autoregression," *in Proceedings of ICCSNT*, Dalian, China, 2019, pp. 380-384.

[15] A. Maryam and B. Keivan, "Using metaheuristic algorithms of genetic, particle swarm optimization and glowworm in the intrusion detection system," *International Journal of Computer Sciences and Networks Security*, Vol. 16, No. 10, 2016, pp. 78-86.

[16] J. Gao, S. Chai, B. Zhang and Y. Xia, "Research on network intrusion detection based on incremental extreme learning machine and adaptive principal component analysis," *Energies*, Vol. 12, No. 7, 2019, pp. 12-23.

[17] T. Zhonghua and Z. Yongquan, "A glowworm swarm optimization algorithm for uninhabited combat air vehicle path planning," *Journal of Intelligent Systems*, Vol. 24, No. 1, 2015, pp. 69-83.

[18] M. Manickam and S. P. Rajagopalan, "A hybrid multi-layer intrusion detection system in cloud," *Cluster Computing*, Vol. 22, No. 2, 2019, pp. 3961-3969.